Electronic transaction system and a transaction terminal adapted for such a system

Field of the invention

5   The invention relates to electronic transaction systems and transaction terminals adapted to perform electronic transaction. An electronic transaction is for example a payment transaction enabling payment of goods at a merchant store or a healthcare transaction enabling a patient to recover fees paid at the doctor, borrowing a book in a library etc...

10

Background of the invention

The payment terminal market is experiencing a price war, and at the same time due to the Europay MasterCard Visa EMV migration, new functionality are required. Further, the telecommunication environment is changing the global architecture of the

15   transaction scheme.

Today, a transaction terminal has all the capabilities and resources to handle a transaction, namely : a PIN pad (keyboard for entering the user Personal Identification Number), a printer, a display, a card reader (either magnetic stripe card or

20   microprocessor card), processing power and memory.

The features required from the transaction terminal are more and more resource demanding. The result is that the processing power and the memory size need to be increased. At the same time the security specifications become more and more severe.

25

Object and summary of the invention

Therefore it is an object of the present invention to provide an electronic transaction system and a transaction terminal adapted for such a system that overcomes the at least one shortcoming of the prior art methods and terminals.

30

The idea of the invention is to leverage on the capabilities of the telecommunication network, mobile telecommunication industry and the fact that processing power is more and more available (e.g. on personal computer PC, personal digital assistant PDA,

mobile phone, or telecommunication router, etc..). According to the invention, instead of having all the resources in one terminal, the resources are distributed as follows :

1) a secured human interface module (Secured PIN Entry Device: SPED) comprising a display, a keypad, a smart card reader and/or a magnetic card reader and possibly a

5   printer,

2) an electronic scheduler (e-scheduler), for example analog to Subscriber Identity Module SIM based, comprising a transaction terminal task manager, ciphering means and merchant contract management means (identification, fees, etc..),

3) a hosting device (PC, mobile phone, PDA, etc ...) having processing means, memory

10   and communication means, and

4) a gateway in the network or a remote server connectable to a service provider (of a bank or a financial institution, of a healthcare institution, etc...).

The gateway have different functionality, for example :

15   - translation of protocols compliant with bank or healthcare institution (message format),

- transaction uploading,

- parameter downloading,

- application boot downloading,

- floor limit management (i.e. a level requiring an authorization for processing the

20   transaction) by card holder,

- data mining capabilities (loyalty programs, data consolidation for multilane merchant applications, local black, gray,.. list management, etc...),

- secure communication with the e-scheduler.

25   Due to the significant decrease of the telecommunication cost, the system according to the invention enables a substantial cost reduction of the price of the transaction terminal.

Brief description of the drawings

30   The following detailed description, given by way of example, will be best understood with the accompanying drawings in which :

- Figure 1 represents schematically an electronic transaction system according to the invention,

- Figure 2 illustrates a particular embodiment of a transaction terminal adapted for a system according to the invention, and

- Figure 3 illustrates different embodiments of a hosting device in an electronic transaction system according to the invention.

Detailed description of the invention

An example of payment transaction involving for example a mobile phone (e.g. compliant with GSM) will be described in more details in relation with Figure 1. A human interface module SPED is connected by a wire or a wire-less connection C1 to a hosting terminal HT, for example a mobile phone. The hosting terminal HT enables to communicate with an application host or virtual terminal server VTS through an existing public or private telecommunication network TN. The virtual terminal server VTS is further able to communicate by adapted communication means and networks C2 with the information processing systems of bank(s) BH.

The human interface module SPED comprises a keypad KP, a display D, a card reader CR, a processing means MP connected to each other by an internal bus B. The human interface module SPED can also comprise a printer P. Advantageously, the human interface module SPED is secured in the sense that it is tamper evident or tamper proof. This means that a user is able to know (for example by seeing that the module was broken) when a fraud tentative to get his PIN is going to occur.

The hosting terminal HT is equipped with a security module or e-scheduler ES. The security module ES is comparable to a Subscriber Identity Module SIM card as currently used in the field of mobile telephony. The hosting means HT is connectable to the human interface module SPED through connection means C1. The processing means and the memory HTR of hosting means can be used by the scheduler means ES for helping in performing various task. The hosting means HT also comprises communication means CR for exchanging data using the telecommunication network TN. A power supply either internal PS, e.g. a battery or external EPS, e.g. electricity network are a source of energy to the hosting terminal HT and also to the human interface module SPED.

The payment terminal comprises the hosting terminal, i.e. the mobile phone, the human interface module SPED and the security module ES. The payment terminal performs the phases of the transaction which involves directly the following actors : the merchant who need to be paid for goods sold or services offered and the customer carrying the

means of payment (a bank or a credit card). The transaction phases comprises the entry of the amount to be paid with the keypad KP, reading and authentication of the bank or credit card through the card reader CR and the processing means MP, entry of the PIN code through the keypad KP, displaying of the instruction to be followed on the

5   display D, possibly editing of payment ticket with the printer P. The human interface module SPED executes these transaction phases under the e-scheduler ES control. However, the human interface module SPED executes totally autonomously the treatments regarding security (display the message asking for PIN code entry, entry of the PIN code, presentation of the PIN code to the card, generation of the ciphered PIN

10   data....).

The communication between the human interface module SPED and the e-scheduler ES through the mobile phone is secured by ciphered data exchange. The cryptographic keys are generated uniquely after a mutual identification of the human interface module SPED and the e-scheduler ES.

15   In an analogous way, the communication between the virtual terminal server VTS and the e-scheduler ES through the mobile phone HT and the telecommunication network TN is secured by mutual identification proceeding and the used of cryptographic keys. The virtual terminal server VTS can comprise a security module EL (e-link) analog to a SIM card. The security module EL can be in relationship with one or more e-

20   scheduler(s). The main task of the security module EL is to allow a secure communication of data between the virtual terminal server VTS and the hosting terminal HT (in the present example the mobile phone).

The e-scheduler uses its host HT (in the present example the mobile phone) to store bulky data without any security requirements connection : e.g. fonts definition, printing

25   format, etc.... The e-scheduler ES and the virtual terminal server VTS contributes to carry out in a distributed way an equivalent of a payment transaction currently carried out on a point-of-sale or payment terminal. A virtual terminal can be seen when considering the addition of all the functionality of the human interface module SPED, the hosting terminal HT including the e-scheduler ES and the virtual terminal server VTS

30   including the security module e-link EL.

The scheduler means ES is specific to the electronic transaction application to be performed for example a banking application, or a healthcare application, etc...

Figure 2 shows a particular embodiment of a transaction terminal adapted for a system according to the invention in which the human interface module SPED and the hosting terminal HT are grouped in one device ATB. This device can be a specific device which include all the functionality of the human interface module SPED and the hosting terminal HT. Alternatively, it can also be for example a personal computer PC, a personal digital assistant PDA, or a mobile phone In all these examples, advantageously, the device is tamper evident or tamper proof, so that a user knows when a fraud tentative to get the user PIN is occurring.

Figure 3 shows schematically different embodiments of a hosting device in an electronic transaction system according to the invention, from top to down of the Figure a personal computer PC, a network hub HUB, a personal digital assistant PDA, and a mobile phone MT respectively. The links shown on the Figure between the different devices/systems/terminals can be wired or wireless. The e-scheduler ES and the security module e-link EL are inserted or connected into the respective devices in an appropriate manner known by the man skilled in the art.

With the system of the invention, it is possible to cheaply adapt the whole system to different type of electronic transaction banking, healthcare, library... simply by changing the scheduler means ES. Also it is possible to use the resources where they are already available, e.g. the hosting terminal or the virtual terminal server (the gateway) while having a basic and cheap but secure human interface module.